WHAT IS CLAIMED IS:

1) A method of determining whether a potential relay device is a relay device, the method comprising:

a) receiving first and second information elements from the potential relay device, wherein the potential relay device is an original source of said second information element; and

b) determining whether a feature of an original source of said first information element and a feature of the potential relay device are features unlikely to relate to a single device,

wherein a positive result of said determining is indicative that the potential relay device is a relay device.

2) The method of claim 1 wherein said second information element is of a type that a relay device of a class of relay devices is unlikely to relay.

3) The method of claim 2 wherein said class of relay devices is selected from the group consisting of a SOCKS proxy, an HTTP proxy using the GET method, an HTTP proxy using the CONNECT method, an IP router and a Network Address Translation device.

4) The method of claim 1 wherein said second information element is part of a communication, wherein the communication is of a type selected from the group consisting of IP, TCP, ICMP, DNS, HTTP, SMTP, TLS, and SSL.

5) The method of claim 1 wherein said first information element is part of a communication, wherein the communication is of a type selected from the group consisting of IP, TCP, ICMP, DNS, HTTP, SMTP, TLS, and SSL.

6) The method of claim 1 wherein said first and said second information elements are parts of a single communication.

7) The method of claim 6 wherein said first and said second information elements are sent in two different layers of a protocol stack.

8) The method of claim 1 wherein said stage of determining comprises:

i) discovering said feature of an original source of said first information element; and

ii) discovering said feature of the potential relay device.

9) The method of claim 8 wherein said stage of determining further comprises:

iii) comparing said feature of an original source of said first information element with said feature of the potential relay device.

10) The method of claim 8 further comprising:

c) obtaining a parameter indicative of said feature of an original source of said first information element; and

d) obtaining a parameter indicative of said feature of the potential relay device.

11) The method of claim 8 wherein said stage of determining further comprises:

iii) considering a time at which at least one of said feature of an original source of said first information element and said feature of the potential relay device, was discovered.

12) The method of claim 1 further comprising:

c) obtaining a parameter indicative of a relationship between said feature of said original source of said first information element and said feature of the potential relay device.

13) The method of claim 12, wherein said stage of determining includes analyzing said parameter indicative of a relationship between said feature of said original source of said first information element and said feature of the potential relay device.

14) The method of claim 12 wherein said parameter is obtained from at least one of said first information element and said second information element.

15) The method of claim 1 further comprising:

c) sending an outgoing communication to at least one of said original source of said first information element and the potential relay device; and

d) Receiving a third information element from said at least one of said original source of said first information element and the potential relay device.

16) The method of claim 15, further including:

e) deriving from said third information element information related to a feature of said at least one of said original source of said first information element and the potential relay device.

17) The method of claim 15 further comprising:

iii) verifying that an original source of said third information element is said original source of said first information element

18) The method of claim 15 further comprising:

iii) verifying that an original source of said third information element is the potential relay device.

19) The method of claim 15 wherein said third information element is selected from the group consisting of an ICMP message, an ICMP Echo Reply message, a DNS query, an HTTP request, an HTTP response, an HTTP 'Server' header, an IP address, a TCP port, a TCP Initial Sequence number, a TCP Initial Window, a WHOIS record, and a reverse DNS record.

20) The method of claim 1 wherein at least one of said feature of an original source of said first information element and said feature of the potential relay device is a feature related to a configuration status.

21) The method of claim 20 wherein said feature related to a configuration status is selected from the group consisting of an operating system type, an operating system version, a software type, an HTTP client type, an HTTP server type, an SMTP client type, an SMTP server type, a time setting, a clock setting and a time zone setting.

22) The method of claim 21 wherein said determining includes examining a parameter indicative of said feature related to a configuration status.

23) The method of claim 21 wherein said parameter is selected from the group consisting of an HTTP 'User-Agent' header, an RFC 822 'X-Mailer' header, An RFC 822 'Received' header, An RFC 822 'Date' header, a protocol implementation manner, a TCP/IP stack fingerprint, an IP address, a TCP port, a TCP initial sequence number, and a TCP initial window.

24) The method of claim 1 wherein at least one of said feature of a source of said first information element and said feature of the potential relay device is a feature related to communication performance.

25) The method of claim 24 wherein said feature related to communication performance is selected from the group consisting of a measured communication

performance, a measured relative communication performance, and an estimated communication performance.

26) The method of claim 24 wherein said feature related to communication performance is selected from the group consisting of a latency of communication, a latency of an incoming communication, a latency of an outgoing communication, a round trip time of a communication, a communication rate, an incoming communication rate, an outgoing communication rate, a maximum communication rate, an incoming maximum communication rate, and an outgoing maximum communication rate.

27) The method of claim 24 wherein said determining includes examining a parameter indicative of said feature related to communication performance.

28) The method of claim 27 wherein said parameter is selected from the group consisting of time of receipt of an information element, time of sending of an information element, a round trip time, a round trip time gap, an IP address, a Whois record, a reverse DNS record, and a rate of acknowledged information.

29) The method of claim 28 wherein a higher round trip time gap is indicative of a higher likelihood that a relay device is being used for malicious purposes.

30) The method of claim 24, wherein said feature related to communication performance is estimated from information about at least one of said original source of said first communication and the potential relay device.

31) The method of claim 30, wherein said information about at least one of said original source of said first communication and the potential relay device is selected from the group consisting of a location of a device, a hostname of a device, and an administrator of a device.

32) The method of claim 1 wherein at least one of said feature of an original source of said first information element and said feature of the potential relay device is selected from the group consisting of a sub-network, an administrator, and a location.

33) The method of claim 32 wherein said determining includes examining a parameter indicative of at least one of said feature of a source of said first communication and said feature of a source of said second communication, and said parameter is selected from the group consisting of an HTTP 'User-Agent'

header, an RFC 822 'X-Mailer' header, an RFC 822 'Received' header, an RFC 822 'Date' Header, an IP address, a WHOIS record, and a reverse DNS record,

34) A method of determining whether a potential relay device is a relay device, the method comprising:

a) receiving first and second information elements from the potential relay device, wherein the potential relay device is an original source of said second information element; and

b) analyzing a configuration status of an original source of at least one of said first and said second information elements, said configuration status selected from the group consisting of an operating system type, an operating system version, a software type, an HTTP client type, an HTTP server type, an SMTP client type, an SMTP server type, a time setting, a clock setting, and a time zone setting. .

35) A method of determining whether a potential relay device is a relay device, the method comprising:

a) receiving first and second information elements from the potential relay device, wherein the potential relay device is an original source of said second information element; and

b) analyzing a feature related to communication performance of an original source of at least one of said first and said second information elements.

36) The method of claim 35, wherein said feature related to communication performance is selected from the group consisting of a latency of communication, a latency of an incoming communication, a latency of an outgoing communication, a round trip time of a communication, a communication rate, an incoming communication rate, an outgoing communication rate, a maximum communication rate, an incoming maximum communication rate, and an outgoing maximum communication rate.

37) A method of determining whether a potential relay device is a relay device, the method comprising:

a) sending a message to an information source device, triggering said information source device to send a DNS request;

b) determining from said DNS request whether said potential relay device is a relay device.

38) A method of determining whether a potential relay device is a relay device, the method comprising:

a) receiving first and second information elements from the potential relay device; and

b) determining whether a feature of an original source of said first information element and a feature of an original source of said second information element are features unlikely to relate to a single device,

wherein a positive result of said determining is indicative that the potential relay device is a relay device.

39) A method of determining whether a potential relay device is a relay device, the method comprising:

a) receiving first and second information elements from the potential relay device, wherein the potential relay device is an original source of said second information element; and

b) checking whether a round-trip time to the potential relay device is significantly different than a round-trip time to an original source of said first information element.

40) A method of determining whether a potential relay device is a relay device, the method comprising:

a) receiving first and second information elements from the potential relay device, wherein the potential relay device is an original source of said second information element; and

b) checking whether an operating system of the potential relay device is different than an operating system of an original source of said first information element.

41) A method of determining whether a potential relay device is a relay device, the method comprising:

a) receiving first and second information elements from the potential relay device, wherein the potential relay device is an original source of said second information element; and

b) checking whether a location of the potential relay device is different than a location of an original source of said first information element.

42) A method of determining whether a potential relay device is a relay device, the method comprising:

a) receiving first and second information elements from the potential relay device, wherein the potential relay device is an original source of said second information element; and

b) checking whether an administrator of the potential relay device is different than an administrator of an original source of said first information element.

43) A method of determining whether a potential relay device is a relay device, the method comprising:

a) determining whether a feature of an original source of a first information element and a feature of the potential relay device are features unlikely to relate to a single device,

wherein the potential relay device is a transmitter of said first information element and of a second information element,

wherein the potential relay device is an original source of said second information element

wherein a positive result of said determining is indicative that the potential relay device is a relay device

44) A system for determining whether a potential relay device is a relay device, the system comprising:

a) an information element receiver, for receiving information elements from a plurality of devices including an information source device and the potential relay device; and

b) a feature incompatibility analyzer, for determining whether a feature of said information source device and a feature of the potential relay device are features unlikely to relate to a single device.

45) The system of claim 44 further comprising:

c) a feature discovery module, for discovering at least one feature selected from the group consisting of a feature of said information source device and a feature of the potential relay device.

46) The system of claim 44, wherein said information element receiver is further configured to receive information elements from a monitored host.

47) The system of claim 44, wherein further comprising:

c) an outgoing information element sender.

48) The system of claim 44, further comprising:

c) a parameter obtainer, for obtaining at least one parameter selected from the group consisting of a parameter indicative of a feature of an information source device, a parameter indicative of a feature of the potential relay device, and a parameter indicative of whether a feature of said information source device and a feature of said potential relay device are features unlikely to relate to a single device.

49) The system of claim 44, further comprising:

c) a feature database for storing a map between pairs of features and data indicative of whether said pairs of features are incompatible features.

50) Computer software, residing on a computer-readable storage medium, comprising instructions for causing a computer to:

a) receive first and second information elements from a potential relay device, wherein the potential relay device is an original source of said second information element; and

b) determine whether a feature of an original source of said first information element and a feature of said potential relay device are features unlikely to relate to a single device,

wherein a positive result of said determining is indicative that said potential relay device is a relay device.